

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
Form PTO-1449 (Modified)
(Use several sheets if necessary)

COMPLETE IF KNOWN

Application Number	10/038,169
Confirmation Number	7811
Filing Date	January 2, 2002
First Named Inventor	Boneh
Group Art Unit	2135
Examiner Name	Bao Tran N To
Attorney Docket No.	36321-8009.US01

Sheet 1 of 5

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.	U.S. Patent or Application		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		NUMBER	Kind Code (if known)			
BT		4,386,416		Giltner	05/31/83	
BT		4,964,164		Fiat, Amos	10/1990	
BT		5,222,133		Chou et al.	10/17/91	
BT		5,557,712		Guay	02/16/94	
BT		5,734,744		Wittenstein	06/07/95	
BT		5,764,235		Hunt et al.	3/25/96	
BT		5,828,832		Holden et al.	10/27/98	
BT		5,848,159		Collins et al.	12/1998	
BT		6,012,198		Anigbogu	02/01/00	
BT		6,073,242		Hardy et al.	06/06/00	
BT		6,081,598		Dai, Wei	06/2000	
BT		6,081,900		Subramaniam et al.	06/2000	
BT		6,098,096		Bayeh et al.	08/01/00	
BT		6,202,157		Brownlie et al.	03/13/01	
BT		6,154,542		Crandall	11/28/00	
BT		6,216,212		Challenger et al.	04/2001	
BT		6,396,926		Takagi, et al.	05/2002	
BT		6,397,330		Elgamal et al.	05/28/02	
BT		6,477,646		Krishna, et al.	11/2002	
BT		6,578,061		Aoki, et al.	06/2003	
BT		6,587,866		Modi et al.	07/01/03	
BT		6,621,505		Beauchamp	09/16/03	
BT		6,757,823		Rao, et al.	06/2004	
BT		6,763,459		Corella, Francisco	07/2004	
BT		6,874,089		Dick et al.	03/2005	
BT		6,886,095		Hind et al.	4/2005	

EXAMINER

/Bao Tran To/

DATE CONSIDERED

08/15/2006

*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
Examiner Name	Bao Tran N To				
Attorney Docket No.	36321-8009.US01				
Sheet	2	of	5		

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No.	U.S. Patent or Application		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		NUMBER	Kind Code (if known)			
BT		6,963,980		Mattsson	11/16/00	
BT		6,990,660		Moshir et al.	1/24/06	
BT	*	10/526,252		Fountain et al.	02-24/05	
BT	*	10/850,827		Koyfman	05/20/04	
BT	*	11/236,046		Metzger et al.	09/26/05	
BT	*	11/236,294		Metzger et al.	09/26/05	
BT	*	11/236,061		Metzger et al.	09/26/05	
BT		2002/0012473		Kondo et al.	9/30/1997	
BT		2002/0073232		Hong et al.	06/13/02	
BT		2002/0112167		Boheh et al.	10/02/02	
BT		2002/0016911		Chawla et al.	07/09/01	
BT		2002/0039420		Schacham et al.	06/08/01	
BT		2002/0066038		Mattsson	11/29/00	
BT		2002/0087884		Shacham et al.	06/08/01	
BT		2003/0014650		Freed et al.	01/16/03	
BT		2003/0065919		Albert et al.	4/2003	
BT		2003/0097428		Afkhami	05/22/03	
BT		2003/0101355		Mattsson	12/28/01	
BT		2003/0123671		He et al.	07/03/03	
BT		2003/0156719		Cronce	02/21/02	
BT		2003/0197733		Beauchamp	09/23/03	
BT		2003/0204513		Bumbulis	10/30/03	
BT		2004/0015725		Boneh et al.	07/24/02	

FOREIGN PATENT DOCUMENTS						
Examiner Initials*	Cite No.	Foreign Patent or Application		Name of Patentee or Applicant of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		Office	NUMBER			
						T

EXAMINER <div style="text-align: center;">/Bao Tran To/</div>	DATE CONSIDERED <div style="text-align: center;">08/15/2006</div>
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
				Examiner Name	Bao Tran N To
Sheet	3	of	5	Attorney Docket No.	36321-8009.US01

FOREIGN PATENT DOCUMENTS								
Examiner Initials*	Cite No.	Foreign Patent or Application			Name of Patentee or Applicant of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
		Office	NUMBER	Kind Code (if known)				
BT	*	WO	01/03398		IBM Corp and IBM UK Limited	01/11/2001		
BT	*	WO	02/101605		Godfrey et al.	12/19/02		

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS				
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.		T
BT	1.	Alteon Web Systems: "The Next Step in Server Loading Balancing" November 1999, Retrieved from the Internet: <u>URL: http://www.nortelnetworks.com/products/library/collateral/intel_int/webworking_wp.pdf</u> , Retrieved on March 2, 2004; pages 4-11.		
BT	2.	Alteon Web Systems: "Networking with the Web in Mind" May 1999, Retrieved from the Internet: <u>URL: http://www.nortelnetworks.com/products/library/collateral/intel_int/webworking_wp.pdf</u> , Retrieved on March 2, 2004; page 1, pages 3-7.		
BT	3.	Boneh, D., "Twenty Years of Attacks on the RSA Cryptosystem," Notices of the AMS, Vol 46, No. 2, pp. 203-213, 1999		
BT	4.	Boneh, et al., "An Attack on RSA Given a Small Fraction of the Private Key Bits," ASIACRYPT '98, LNCS 1514, pp. 25-34, 1998		
BT	5.	Boneh, et al., "Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$," (extended abstract), 1999		
BT	6.	Boneh, et al., "Efficient Generation of Shared RSA Keys," (extended abstract)		
BT	7.	Durfee, G., et al., "Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacypt '99," ASIACRYPT 2000, LNCS 1976, pp. 14-29, 2000		
BT	8.	Fiat, A. "Batch RSA, (digital signatures and public key krypto-systems)" Advances in Cryptology - Crypto '89 Proceedings 20-24 August, 1989, Springer-Verlag		
BT	9.	Großschädl, J., et al., "The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip," 2000		

EXAMINER	/Baotran To/	DATE CONSIDERED	08/15/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
Examiner Name	Bao Tran N To				
Sheet	4	of	5	Attorney Docket No.	36321-8009.US01


OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
BT	10.	Herda, S., "Non-repudiation: Constituting evidence and proof in digital cooperation," Computer Standards and Interfaces, Elsevier Sequoia, Lausanne, CH, 17:1 (69-79) 1995.	
BT	11.	Immerman, N., "Homework 4 with Extensive Hints," 2000	
BT	12.	Menezes, A., et al., "Handbook of Applied Cryptography," 1996 CRC Press, pp. §8.2-8.3 and §14.5	
BT	13.	Netscape; "Netscape Proxy Server Administrator's Guide, Version 3.5 for Unix"; February 25, 1998; Retrieved from the Internet.	
BT	14.	Oppliger, R.; "Authorization Methods for E-Commerce Applications"; 1999	
BT	15.	RSA Laboratories: "PKCS #7: Cryptographic Message Syntax Standard, Version 1.5," RSA Laboratories Technical Note, pp. 1-30, November 1, 1993.	
BT	16.	RSA "PKCS #1 v2.0 Amendment 1: Multi-Prime RSA," 2000	
BT	17.	"Security Protocols Overview (An RSA Data Security Brief)", RSA Data Security, 1999, http://www.comms.scitech.susx.ac.uk/fft/crypto/security_protocols.pdf , pages 1-4.	
BT	18.	Schacham, H., et al., "Improving SSL Handsake Performance via Batching," Topics in Cryptology, pp. 28-43, 2001.	
BT	19.	Shand, M., et al., "Fast Implementations of RSA Cryptography," 1993	
BT	20.	Sherif, M.H., et al., "SET and SSL: Electronic Payments on the Internet," IEEE, pp. 353-358 (1998)	
BT	21.	Stallings, W., "IP Security," Network Security Essentials, Applications and Standards, Chapters 6 and 7, pp. 162-223, 2000	
BT	22.	Takagi, T., "Fast RSA-Type Cryptosystem Modulo p^kq ," 1998	

EXAMINER	/Baotran To/	DATE CONSIDERED	08/15/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
Examiner Name	Bao Tran N To				
Sheet	5	of	5	Attorney Docket No.	36321-8009.US01

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
BT	23.	Takagi, T., "Fast RSA-Type Cryptosystems Using N-Adic Expansion," Advances in Technology – CRYPTO '97, LNCS 1294, pp. 372-384, 1997	
BT	24.	Wiener, M., "Cryptanalysis of Short RSA Secret Exponents," 1989	

EXAMINER	/Baotran To/	DATE CONSIDERED	08/15/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance <u>and</u> not considered. Include copy of this form with next communication to application(s).			

 INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
				Examiner Name	Bao Tran N To
Attorney Docket No.	36321-8009.US01				
Sheet	1	of	6		

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No.	U.S. Patent or Application		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		NUMBER	Kind Code (if known)			
BT	A1.	4,386,416		Giltner	5/31/1983	
	A2.	4,964,164		Fiat, Amos	10/16/1990	
	A3.	5,222,133		Chou et al.	6/22/1993	
	A4.	5,557,712		Guay	9/17/1996	
	A5.	5,734,744		Wittenstein	3/31/1998	
	A6.	5,764,235		Hunt et al.	6/9/1998	
	A7.	5,828,832		Holden et al.	10/27/1998	
	A8.	5,848,159		Collins et al.	12/8/1998	
	A9.	6,021,198		Anigbogu	2/1/2000	
	A10.	6,073,242		Hardy et al.	6/6/2000	
	A11.	6,081,598		Dai, Wei	6/27/2000	
	A12.	6,081,900		Subramaniam et al.	6/27/2000	
	A13.	6,094,485		Weinstein, et al.	7/25/2000	
	A14.	6,098,093		Bayeh et al.	8/1/2000	
	A15.	6,098,096		Tsirigotis et al.	8/1/2000	
	A16.	6,154,542		Crandall	11/28/2000	
	A17.	6,202,157		Brownlie et al.	3/13/201	
BT	A18.	6,216,212		Challenger et al.	4/10/2001	

EXAMINER <div style="text-align: center;">/Baotran To/</div>	DATE CONSIDERED <div style="text-align: center;">08/15/2006</div>
<small>*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).</small>	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
Examiner Name	Bao Tran N To				
Sheet	2	of	6	Attorney Docket No.	36321-8009.US01

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No.	U.S. Patent or Application		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		NUMBER	Kind Code (if known)			
BT	A19.	6,233,577		Ramasubramani et al.	5/15/2001	
	A20.	6,396,926		Takagi, et al.	5/28/2002	
	A21.	6,397,330		Elgamal et al.	5/28/2002	
	A22.	6,473,802		Masters	10/29/2002	
	A23.	6,477,646		Krishna, et al.	11/5/2002	
	A24.	6,502,135		Munger et al.	12/31/2002	
	A25.	6,519,365		Kondo et al.	2/11/2003	
	A26.	6,578,061		Aoki, et al.	6/10/2003	
	A27.	6,584,567		Bellwood et al.	6/24/2003	
	A28.	6,587,866		Modi et al.	7/1/2003	
	A29.	6,615,276		Mastrianni et al.	9/2/2003	
	A30.	6,621,505		Beauchamp et al.	9/16/2003	
	A31.	6,678,733		Brown et al.	1/13/2004	
	A32.	6,681,327		Jardin, Cary A.	1/20/2004	
	A33.	6,694,323		Bumbulis	2/17/2004	
	A34.	6,751,677		Ilkicky et al.	6/15/2004	
	A35.	6,757,823		Rao et al.	6/29/2004	
BT	A36.	6,763,459		Corella, Francisco	7/13/2004	

EXAMINER	DATE CONSIDERED
/Baotran To/	08/15/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
Examiner Name	Bao Tran N To				
Sheet	3	of	6	Attorney Docket No.	36321-8009.US01

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No.	U.S. Patent or Application		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		NUMBER	Kind Code (if known)			
BT	A37.	6,874,089		Dick et al.	3/29/2005	
	A38.	6,886,095		Hind et al.	4/26/2005	
	A39.	6,915,427		Maruyama et al.	7/5/2005	
	A40.	6,941,459		Hind et al.	9/6/2005	
	A41.	6,963,980		Mattsson	11/5/2005	
	A42.	6,990,636		Beauchamp	1/24/2006	
	A43.	6,990,660		Moshir et al.	1/24/2006	
	A44.	10/526,252		Fountain et al. 8024	2/24/2005	
	A45.	11/236,046		Metzger et al. 8033	9/26/2005	
	A46.	11/236,061		Metzger et al. 8035	9/26/2005	
	A47.	11/236,294		Metzger et al. 8034	9/26/2005	
	A48.	11/341,060		Metzger et al. 8036	1/27/06	
	A49.	2002/0016911		Chawla et al.	2/7/2002	
	A50.	2002/0039420		Schacham et al.	4/4/2002	
	A51.	2002/0066038		Mattsson	5/30/2002	
	A52.	2002/0073232		Hong et al.	6/13/2002	
	A53.	2002/0087884		Schacham et al.	7/4/2002	
BT	A54.	2003/0014650		Freed et al.	1/16/2003	

EXAMINER	DATE CONSIDERED
/Baotran To/	08/15/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
Examiner Name	Bao Tran N To				
Sheet	4	of	6	Attorney Docket No.	36321-8009.US01

U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No.	U.S. Patent or Application		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		NUMBER	Kind Code (if known)			
BT	A55.	2003/0065919		Albert et al.	4/3/2003	
BT	A56.	2003/0097428		Afkhami	5/22/2003	
BT	A57.	2003/0101355		Mattsson	5/29/2003	
BT	A58.	2003/0123671		He at al.	7/3/2003	
BT	A59.	2003/0156719		Cronce	8/21/2003	
BT	A60.	2004/0015725		Boneh et al.	1/22/2004	
BT	A61.	2006/0041533		Koyfman	2/23/2006	
BT	A62.	2006/0149962		Fountain et al.	7/6/2006	

FOREIGN PATENT DOCUMENTS								
Examiner Initials*	Cite No.	Foreign Patent or Application			Name of Patentee or Applicant of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
		Office	NUMBER	Kind Code (if known)				
BT	B1.	WO	01/03398		IBM Corp and IBM UK Limited	01/11/2001		
BT	B2.	WO	02/101605		Research In Motion Limited	12/19/02		

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
BT	C1.	Alteon Web Systems: "The Next Step in Server Loading Balancing" November 1999, Retrieved from the Internet: URL: http://www.nortelnetworks.com/products/library/collateral/intel_int/webworking_wp.pdf , Retrieved on March 2, 2004; pages 4-11.	
BT	C2.	Alteon Web Systems: "Networking with the Web in Mind" May 1999, Retrieved from the Internet: URL: http://www.nortelnetworks.com/products/library/collateral/intel_int/webworking_wp.pdf , Retrieved on March 2, 2004; page 1, pages 3-7.	

EXAMINER	/Bao Tran To/	DATE CONSIDERED	08/15/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).			

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
Examiner Name	Bao Tran N To				
Sheet	5	of	6	Attorney Docket No.	36321-8009.US01

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
BT	C3.	Boneh, D., "Twenty Years of Attacks on the RSA Cryptosystem," Notices of the AMS, Vol 46, No. 2, pp. 203-213, 1999	
BT	C4.	Boneh, et al., "An Attack on RSA Given a Small Fraction of the Private Key Bits," ASIACRYPT '98, LNCS 1514, pp. 25-34, 1998	
BT	C5.	Boneh, et al., "Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$," (extended abstract), 1999	
BT	C6.	Boneh, et al., "Efficient Generation of Shared RSA Keys," (extended abstract)	
BT	C7.	Durfee, G., et al., "Cryptanalysis of the RSA Schemes with Short Secret Exponent from Asiacrypt '99," ASIACRYPT 2000, LNCS 1976, pp. 14-29, 2000	
BT	C8.	Fiat, A. "Batch RSA, (digital signatures and public key krypto-systems)" Advances in Cryptology – Crypto '89 Proceedings 20-24 August, 1989, Springer-Verlag	
BT	C9.	Großschädl, J., et al., "The Chinese Remainder Theorem and its Application in a High-Speed RSA Crypto Chip," 2000	
BT	C10.	Herda, S., "Non-repudiation: Constituting evidence and proof in digital cooperation," Computer Standards and Interfaces, Elsevier Sequoia, Lausanne, CH, 17:1 (69-79) 1995.	
BT	C11.	Immerman, N., "Homework 4 with Extensive Hints," 2000	
BT	C12.	Menezes, A., et al., "Handbook of Applied Cryptography," 1996 CRC Press, pp. §8.2-8.3 and §14.5	
BT	C13.	Netscape; "Netscape Proxy Server Administrator's Guide, Version 3.5 for Unix"; February 25, 1998; Retrieved from the Internet.	
BT	C14.	Oppliger, R.; "Authorization Methods for E-Commerce Applications"; 1999	
BT	C15.	RSA Laboratories: "PKCS #7: Cryptographic Message Syntax Standard, Version 1.5," RSA Laboratories Technical Note, pp. 1-30, November 1, 1993.	

EXAMINER	DATE CONSIDERED
/Baotran To/	08/15/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT Form PTO-1449 (Modified) (Use several sheets if necessary)				COMPLETE IF KNOWN	
				Application Number	10/038,169
				Confirmation Number	7811
				Filing Date	January 2, 2002
				First Named Inventor	Boneh
				Group Art Unit	2135
Examiner Name	Bao Tran N To				
Sheet	6	of	6	Attorney Docket No.	36321-8009.US01

OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume issue number(s), publisher, city and/or country where published.	T
BT	C16.	RSA "PKCS #1 v2.0 Amendment 1: Multi-Prime RSA," 2000	
BT	C17.	"Security Protocols Overview (An RSA Data Security Brief)", RSA Data Security, 1999, http://www.comms.scitech.susx.ac.uk/fft/crypto/security_protocols.pdf , pages 1-4.	
BT	C18.	Schacham, H., et al., "Improving SSL Handsake Performance via Batching," Topics in Cryptology, pp. 28-43, 2001.	
BT	C19.	Shand, M., et al., "Fast Implementations of RSA Cryptography," 1993	
BT	C20.	Sherif, M.H., et al., "SET and SSL: Electronic Payments on the Internet," IEEE, pp. 353-358 (1998)	
BT	C21.	Stallings, W., "IP Security," Network Security Essentials, Applications and Standards, Chapters 6 and 7, pp. 162-223, 2000	
BT	C22.	Takagi, T., "Fast RSA-Type Cryptosystem Modulo p^kq ," 1998	
BT	C23.	Takagi, T., "Fast RSA-Type Cryptosystems Using N-Adic Expansion," Advances in Technology – CRYPTO '97, LNCS 1294, pp. 372-384, 1997	
BT	C24.	Wiener, M., "Cryptanalysis of Short RSA Secret Exponents," 1989	

EXAMINER	DATE CONSIDERED
/Baotran To/	08/15/2006
*EXAMINER: Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to application(s).	